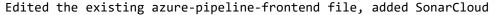
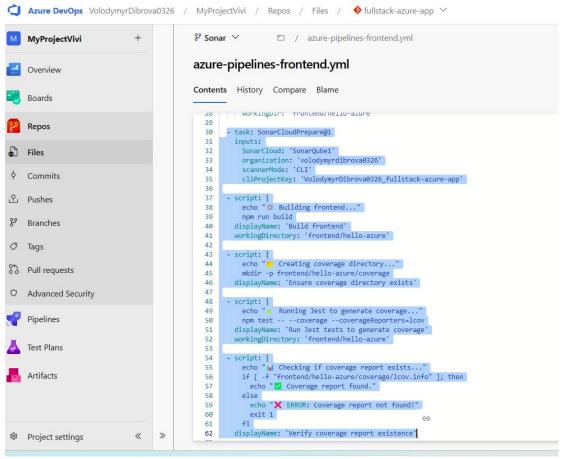
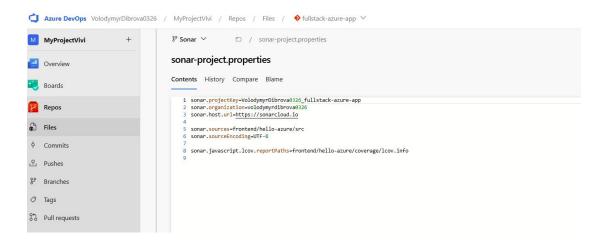
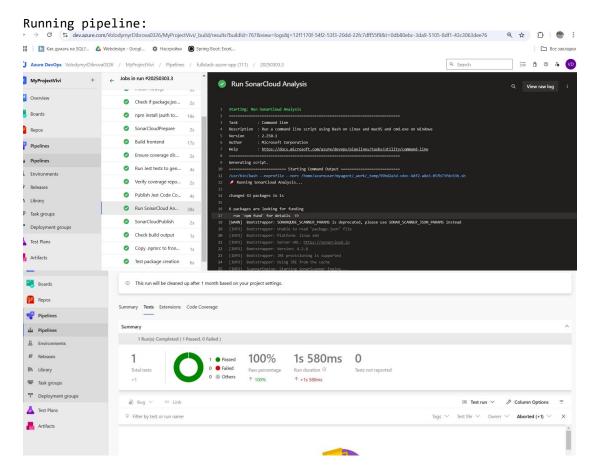
Task 1: Implementing Basic Security Scans in Azure Pipelines



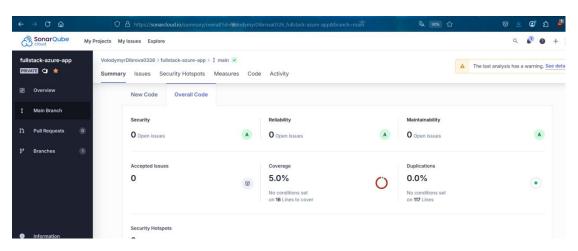


#### Created sonar-project.properties





## Result after SonarQube



2.

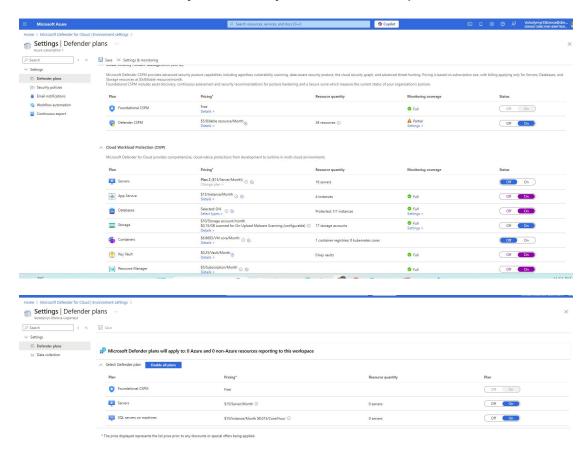
Task 2: Integrating Azure Security Center with DevOps Workflows Objective: Configure Azure Security Center to monitor resources and integrate its alerts

into Azure DevOps workflows for automated security incident response.
Steps:

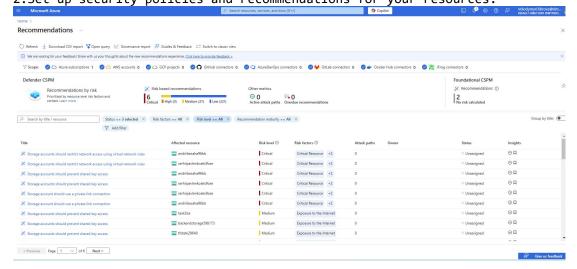
- Enable Azure Security Center in your Azure subscription.
- Set up security policies and recommendations for your resources.• Configure alerts for security incidents and integrate them with Azure DevOps using

Azure Logic Apps or Azure Functions.

- Create an Azure DevOps work item automatically when a security alert is triggered.
- Test the integration by simulating a security incident and verifying that the workflow responds appropriately.
- 1. Enabled Azure Security Center in your Azure subscription.

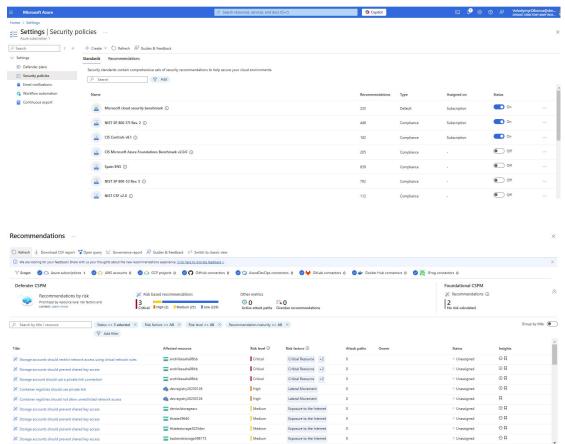


2.Set up security policies and recommendations for your resources.

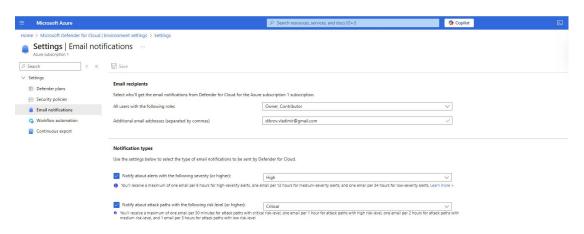


 $\cdot$  CIS Microsoft Azure Foundations Benchmark (v2.0.0) – provides advanced security recommendations.

- NIST SP 800-53 Rev. 5 security standard for regulatory compliance.
- · CIS Controls v8.1 general security practices.

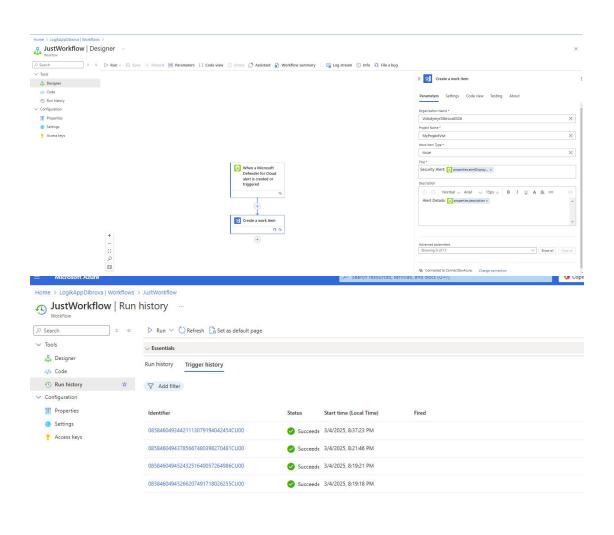


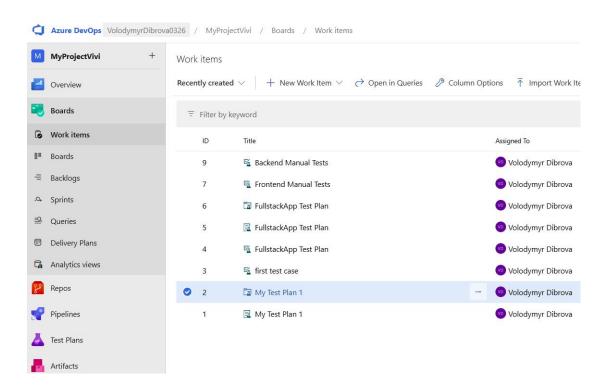
3.Configured alerts for security incidents and integrate them with Azure DevOps using



Azure Logic Apps or Azure Functions.

 $\bullet$  Create an Azure DevOps work item automatically when a security alert is triggered.





# Task 3: Implementing a Comprehensive DevSecOps Strategy with Azure Policy and

#### **Automation**

**Objective:** Implement a comprehensive DevSecOps strategy using Azure Policy, Azure

Blueprints, and automation to enforce security best practices, ensure compliance, and

streamline governance across your Azure environments.

#### Steps:

#### • Create Azure Policies:

Navigate to the Azure Portal and go to "Policy." Create or select existing policies that

enforce security best practices, such as requiring encryption at rest, ensuring

secure network configurations, or enforcing tag usage for resources. Assign these

policies to your Azure subscriptions or resource groups to start auditing resources

for compliance.

### • Set Up Azure Blueprints:

In the Azure Portal, go to "Blueprints." Create a new blueprint definition that includes

your Azure Policies, resource templates, and RBAC assignments. Publish and assign

the blueprint to your target subscriptions to ensure consistent deployment of

resources and policies.

#### • Automate Compliance Monitoring:

Use Azure Monitor to set up alerts for policy compliance states. Configure Log

Analytics to collect and analyze data on policy compliance, creating dashboards to

visualize this data.

# • Implement Automated Remediation:

Use Azure Automation or Azure Functions to create runbooks or scripts that automatically remediate common policy violations, such as enabling encryption or

applying missing tags. Trigger these runbooks based on alerts from Azure Monitor

when policy violations are detected.

#### • Configure Role-Based Access Control (RBAC):

Go to "Access control (IAM)" in the Azure Portal for your resources. Assign roles that

adhere to the principle of least privilege, ensuring users have only the permissions they need. Regularly review role assignments and adjust as necessary based on access requirements.

#### • Integrate with Azure DevOps:

Set up Azure DevOps pipelines to include policy compliance checks using Azure CLI

or Azure PowerShell tasks. Use these tasks to ensure that resources deployed

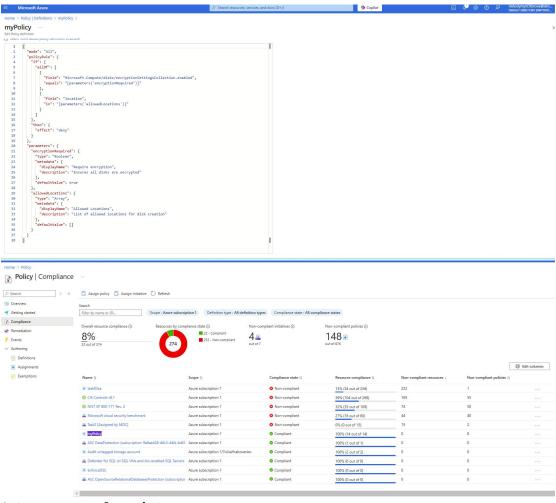
through the pipeline are compliant with your defined policies.

# • Test and Validate the Implementation:

Deploy a test resource using your blueprint and verify that all policies are applied

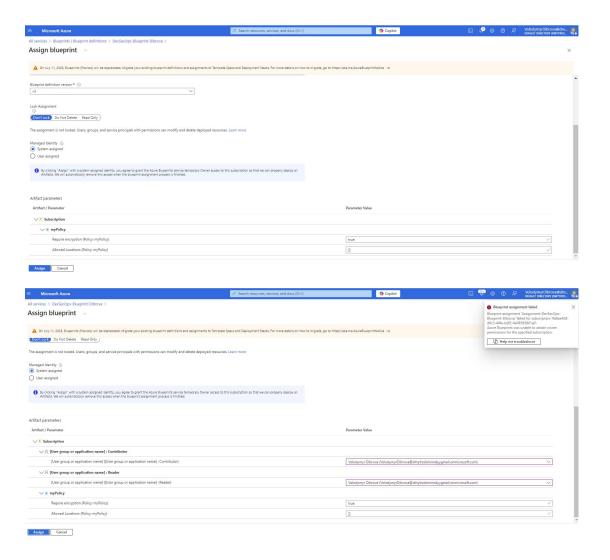
and compliant. Simulate a policy violation and test the automated remediation process to ensure it works as expected.

# Create Azure Policies and Assigned



# Set Up Azure Blueprints





Issue: I cannot continue the task because I don't have Contibutor permissions on the subscription. Azure Blueprints requires Contibutor access to assign policies and deploy resources. Without this permission, the assignment fails.